AMENDMENTS TO THE CLAIMS

1. (Canceled).

2. (Previously Presented) The method of claim 3 further wherein transferring comprises transferring a number of bytes specified by an operand from a memory.

3. (Currently Amended) A method comprising

receiving, by a processor, an instruction to launch a code module to establish a trusted system environment;

verifying, by the processor in response to receiving the instruction, that the environment of the processor is appropriate to launch the code module;

updating, by the processor in response to verifying that the environment of the processor is appropriate, event processing to support launching the code module;

locking, by the processor in response to updating event processing, a processor bus coupling the processor to other processors;

configuring, by the processor in response to locking the processor bus, a cache memory of a processor to operate in a private mode in which requests within the memory range of the cache are satisfied by the cache and cache lines are not replaced or invalidated in response to snoop requests on the processor bus;

transferring, by the processor in response to configuring the cache memory to operate in the private mode, the ~~an authenticated~~ code module to the cache memory;

~~authenticating~~ determining, by the processor in response to transferring the code module to the cache memory, that the code module stored in the cache memory is authentic; and

executing the ~~authenticated~~ code module from the cache memory in response to determining that the ~~authenticated~~ code module is authentic~~; and~~

~~reconfiguring the cache memory to operate in a mode in which cache lines are replaced in response to cache misses~~.

4. (Previously Presented) The method of claim 3 further comprising invalidating the cache memory prior to storing the code module in the cache memory.

5. (Canceled).

6. (Previously Presented) The method of claim 3 further comprising determining whether the code module is authentic based upon a digital signature of the code module.

7. (Previously Presented) The method of claim 3 further comprising

obtaining a first value from the code module stored in the cache memory;

computing a second value from the code module; and

determining that the code module is authentic in response to the first value and the second value having a predetermined relationship.

8. (Previously Presented) The method of claim 3 further comprising

retrieving a key,

decrypting a digital signature of the code module with the key to obtain a first value,

hashing the code module to obtain a second value; and

executing the code module in response to the first value and the second value having a predetermined relationship.

9. (Previously Presented) The method of claim 8 wherein decrypting comprises using the key to RSA-decrypt the digital signature, and hashing comprises apply a SHA-1 hash to the code module to obtain the second value.

10. (Original) The method of claim 8 further comprising retrieving the key from the processor.

11. (Original) The method of claim 8 further comprising retrieving the key from a chipset.

12. (Previously Presented) The method of claim 8 further comprising retrieving the key from a token.

13. (Previously Presented) The method of claim 3 wherein transferring comprises receiving the code module from a machine readable medium.

14-34. (Canceled).